AFRL-RI-RS-TR-2011-094

QUANTUM SIMULATION BEYOND STABILIZER FORMALISM

UNIVERSITY OF MICHIGAN

MAY 2011

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■**UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2011-094 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/	/s/
PAUL ALSING Work Unit Manager	MICHAEL J. HAYDUK, Acting Chief Computing & Communications Division Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
May 2011	Final Technical Report	October 2009 – October 2010

4. TITLE AND SUBTITLE

QUANTUM SIMULATION BEYOND STABILIZER FORMALISM

5a. CONTRACT NUMBER FA8750-10-2-0016

5b. GRANT NUMBER N/A

5c. PROGRAM ELEMENT NUMBER 62788F

6. AUTHOR(S)

Igor Markov

5d. PROJECT NUMBER T2AQ

5e. TASK NUMBER QS

5f. WORK UNIT NUMBER SF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

University of Michigan
Computer Science & Engineering
2260 Hayward Avenue
Ann Arbor, MI 48109-2121

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RITC
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RI

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

AFRL-RI-RS-TR-2011-094

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. PA# 88ABW-2011-2387.
Date Cleared: 29 APRIL 2011.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This is the final report for a one-year project on Quantum Circuit Simulation Beyond the Stabilizer Formalism. The project included the development of new mathematical and algorithmic concepts for the efficient simulation of quantum circuits and their implementation in software. In particular, the algorithms we develop extend the stabilizer formalism for simulating a restricted set of quantum circuits - the extensions apply to any given quantum circuit, but computational cost may be significant. Our research therefore put special emphasis on ensuring computational efficiency. The software we developed provided infrastructure for compiling quantum programs into quantum circuits, which can then be simulated.

15. SUBJECT TERMS

Quantum information processing, quantum simulation, stabilizer circuits

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON / 19b. TELEPHONE NUMBER (*Include area code*)
U	U	U	UU	13	PAUL ALSING / N/A

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Table of Contents

Table of Figures

1. Summary

This project focuses on innovative technologies for information processing based on quantum Physics. The project's operational objective is to enhance simulation of quantum circuits containing many, but not all stabilizer gates. Such circuits result when enriching arbitrary quantum circuits with quantum error-correction codes. The project's technical objective is the design of algorithms that extend techniques by Aaronson & Gottesman [1] for stabilizer gates, based on the Heisenberg representation of quantum computers. This is accomplished by decomposing each quantum non-stabilizer gate into a linear combination of stabilizer gates, simulating each resulting stabilizer gate in a separate thread, and reassembling the threads. The threads can be implemented using parallel or using sequential computation. The key issue in our research is handling the exponential increase in the number of threads, through data reuse.

The project's main accomplishments include the following:

1. A general simulation framework that maintains orthogonal superpositions of stabilizer states and supports both unitary gates and measurements.
2. A technique to apply unitary non-stabilizer gates by decomposing them into linear combinations of unitary stabilizer gates.
3. Techniques to compress superpositions of stabilizer states, using the inner-product operation.
4. A series of results describing the geometry of stabilizer states, including pairs of orthogonal stabilizer states and nearest neighbors, as well states that are far from any stabilizer states.
5. A software architecture for compiling quantum programs into quantum circuits that can be simulated by a stand-alone software tool.

2. Introduction

The work reported includes algorithmic techniques and methodologies to simulate quantum ciruicts with improved efficiency. Its key objective is to develop and evaluate new principles, algorithms and software for high-performance simulation of quantum circuits – a widely accepted computational model for quantum computation and communication

Technology background The construction of computer algorithms and software models that simulate physical systems plays a fundamental role in all branches of science and engineering, and plays a special role in attempts to achieve competitive advantage over non-quantum techniques. In particular, it was observed in the 1980s that the important task of simulating quantum-mechanical processes on a standard computer requires an extraordinary amount of computer memory and runtime. Such observations gave rise to the notion of quantum computing, where quantum mechanics itself is used to simulate naturally-occurring quantum properties and phenomena. The key insight is to replace the familiar 0 and 1 bits of conventional computing with information units called qubits (quantum bits) that capture quantum states of elementary particles or atomic nuclei. By operating on qubits, a quantum computer can, in principle, process exponentially more data than a classical computer in a similar number of steps. Existing quantum algorithms exponentially outperform best known techniques for key tasks in code-breaking. In addition to quantum computation, quantum communication exhibits unique properties, such as automatic detection of attempts to eavesdrop. High-speed quantum communication systems have been built in the early and mid 2000s by National Institute of Standards and Technology, several DARPA contractors (notably, BBN Technologies) and start-ups in the US and Europe. Some of these systems are currently available commercially, and others are operated 24x7 for research purposes and as testbeds for network protocol development. The most serious fundamental obstacle to the practical quantum information processing known today is the inherent instability of qubits. This obstacle is traditionally addressed by quantum error-correction techniques, which are generally available but require significant overhead and require adaptation to individual quantum circuits. In order to scale quantum information processing, including computation and communication, to large and complex systems, quantum device operation is compactly captured by the abstract formalism of quantum circuits. These circuits consist of interconnected quantum gates that act on qubits. They can be composed in a hierarchical manner, using design techniques similar to those used in digital logic design. However, as quantum circuits offer a much broader range of information-processing possibilities, their design and evaluation entail a dramatic increase of complexity, requiring new levels of sophistication in design algorithms and tools. A particularly important class of design tools performs simulation of quantum circuits on conventional workstations, i.e., these tools produce representative outputs of ideal quantum circuits on particular inputs, but without requiring quantum hardware.

Quantum simulation tools typically consist of a front-end and a back-end. The front-end facilitates the development of quantum software and the back-end acts as a temporary replacement of (hardware) quantum processing units to run such software. Once quantum hardware is available, it can be used in conjunction with pre-existing front-end to run the accumulated software with increased efficiency. In some cases, quantum simulation can demonstrate that certain quantum software does not bring competitive advantage to quantum hardware over conventional CPUs. This project develops new mathematical and algorithmic concepts for efficient simulation of quantum circuits. These concepts are being implemented in software and will help evaluating architectures for error-corrected quantum communication and computation.

Project Participants

Current graduate student at the University of Michigan: Héctor García, Armin Alaghi

Faculty at the University of Michigan: Prof. John Hayes, Prof. Igor Markov

Other participants: Dr. Ilia Polian (University of Freiburg), Prof. Shigeru Yamashita (Ritsumeikan University)

3. Methods and Procedures

The computational complexity of simulating quantum-mechanical phenomena on conventional computers has been one of the first questions studied in quantum information processing. The apparent intractability of generic quantum simulation suggested the idea of using quantum phenomena to accelerate computation. The speed-ups offered by Shor's quantum factoring algorithm and Grover's quantum search algorithm over their corresponding classical formulations helped fuel interest and expectations in this area. Most quantum algorithms are described in terms of quantum circuits and, just like conventional digital circuits, require functional simulation to determine the best design choices given limited resources. Several software packages have been developed to simulate generic quantum circuits including Oemer's Quantum Computation Language (QCL), and Viamontes' Quantum Information Decision Diagrams (QuIDD) QuIDDPro software. These simulators feature a classical programming model coupled with a computational interface for quantum circuits. While QCL simulates quantum circuits directly using state vectors, QuIDDPro uses a variant of binary decision diagrams to store state vectors more compactly in some cases. Since the size of the state vector scales exponentially in the number of qubits, such general-purpose simulators can only simulate a relatively small number of qubits.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Figure 1. Controlled-NOT, Hadamard and Phase gates.

Gottesman and Knill [2] showed that, for certain types of non-trivial quantum circuits known as stabilizer circuits, efficient simulation on classical computers is possible. Stabilizer circuits are exclusively composed of stabilizer gates {Controlled-NOT, Hadamard and Phase gates} (Figure 1) followed by one-qubit measurements in the computational basis. Such circuits are applied to a computational basis state and produce output states known as stabilizer states. The case of purely unitary stabilizer circuits (without measurement gates) is considered often, e.g., by consolidating measurements at the end. Stabilizer circuits can be simulated in poly-time by keeping track of the Pauli matrices that stabilize the quantum state. Because of their extensive applications in quantum error-correction codes (QECC), stabilizer circuits have been studied extensively. A simulation technique dealing directly with stabilizer states will use at least $O(n^2)$ memory. Aaronson and Gottesman [1] proposed an improved simulation technique that uses a bit-vector representation to simulate stabilizer circuits.

Vidal [3] established a necessary condition for a quantum algorithm to defy efficient classical simulation. This condition demands that the amount of entanglement generated by the algorithm on n qubits grow faster than log(n). In other words, if an algorithm does not generate sufficiently high entanglement, it can be simulated efficiently. Since stabilizer states can be maximally entangled, entangled states are not sufficient to prevent efficient simulation. By extending stabilizer simulation, we seek to simulate new classes of entangled states and circuits that generate them. We also seek classes of states that cannot be simulated this way and may therefore suggest new types of quantum speed-ups.

Current techniques for simulating stabilizer circuits offer efficient algorithms but make the following assumptions: (i) the initial state of the quantum system must be a computational-basis or stabilizer state and (ii) the quantum gates that are applied to the system must be stabilizer gates. Relaxing these constraints provides a means for generalizing stabilizer simulation. To relax the first constraint, we consider almost-stabilizer circuits, i.e., circuits that contain a small number of non-stabilizer gates. Decompositions of non-stabilizer gates into stabilizer gates allow us to design flexible simulation techniques that leverage fast simulation of stabilizer gates while not restricting the types of gates that can be simulated. To this end, we developed a data structure that uses non-stabilizer gate decompositions to simulate almost-stabilizer circuits with runtime polynomial in the number of stabilizer gates and exponential in the number of non-stabilizer gates. The second constraint is relaxed by admitting a stabilizer decomposition that specifies a non-stabilizer state as a linear combination of stabilizer states. It is important to note that given two physical quantum states, there is no quantum-mechanical operation to combine them in a linear combination – such operations are specific to the simulation context. Generic simulation algorithms typically can process arbitrary linear combinations, but algorithms that are limited to certain quantum states usually have trouble with linear combinations. Therefore, we seek compact decompositions of non-stabilizer states into stabilizer states and design compatible simulation techniques.

4. Results and Discussion

We report the following results on beyond-stabilizer simulation of quantum circuits.

(i) We define a canonical representation for stabilizer states and design relevant algorithms to obtain such a representation from an arbitrary set of independent Pauli stabilizers.

(ii) We prepare tables of all 1-qubit, 2-qubit, 3-qubit stabilizer states, and calculate their angles with the ground state.

(iii) We prove important properties that describe the geometry of stabilizer states including nearest neighbors and the relationship between orthogonality and the Pauli generators of a stabilizer state.

(iv) We prove that a particular class of quantum states cannot be approximated with arbitrary precision using poly-sized superpositions of stabilizer states.

(v) We leverage the theoretical insights by Aaronson and Gottesman to design an algorithm that uses circuit synthesis to compute the inner product between stabilizer states.

(vi) We propose an algorithm for calculating an upper bound on the inner product between stabilizer states, which avoids circuits synthesis and determines whether two stabilizer states are equivalent.

(vii) We propose several algorithms to restructure and compress large superpositions of stabilizer states arising during “beyond-stabilizer" simulation.

(viii) We propose an overall simulation flow for stabilizer-based simulation of generic quantum circuits. Our flow emphasizes efficiency and flexibility by leveraging our restructuring techniques for superpositions of stabilizer states.

(ix) We propose to adapt well-known distributed computing techniques to design a parallel implementation of our simulation flow.

Detailed descriptions of these contributions are given in [1], which we delivered to AFRL. This document also (1) reviews the stabilizer formalism necessary to understand the technical details of our contributions, and (2) outlines open challenges. In addition to above contributions, we have developed software infrastructure for compiling quantum programs into quantum circuits, and for designing stand-alone software tools that operate on such circuits. In ongoing work, this infrastructure supports high-performance circuit simulators.

5. Conclusions

The stabilizer formalism was generalized by Aaronson and Gottesman to include simulation of non-stabilizer gates, but this generalization is missing a number of components necessary for a practical implementation. These components have been developed in our work, which lays the foundation for high-performance simulation of quantum circuits dominated by stabilizer gates.

Acknowledgements

Contractor acknowledges Government's support in the publication of this report. This material is based upon work funded by AFRL, under AFRL Contract No. FA8750-10-2-0016. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of AFRL.

6. List of Abbreviations and Acronyms

AFRL	Air Force Research Laboratory
CNOT	Controlled-Not
CPU	Central Processing Unit
DARPA	Defense Advanced Research Projects Agency
QCL	Quantum Computation Language
QECC	Quantum Error Correction Codes
Qubit	quantum bit
QuIDD	Quantum Information Decision Diagram

7. References

[1] S. Aaronson and D.Gottesman, “Improved simulation of stabilizer circuits,: Phys. Rev. A 70, 052328 (2004).

[2] D. Gottesman, “Stabilizer codes and quantum error correction,” quant-ph/970502, CalTech Ph.D. Thesis.

[3] G. Vidal, “Efficient classical simulation of slightly entangled quantum computation,” Phys. Rev. Lett. **91**, 147902 (2003).

Appendix A. Publications

This list includes publications developed under earlier funding from AFRL.

[4] H. J. Garcia and I.L. Markov, “The Hitchhiker’s Guide to the Stabilizer Formalism”, *draft*, 2010.